日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　１月２４日

出願番号
Application Number: 特願２００１－０１６１５５

出願人
Applicant(s): ケープレックス・インク

２００１年　７月　２日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０６２０９７

【書類名】　特許願
【整理番号】　001873
【提出日】　平成13年 1月24日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/00
【発明者】
　【住所又は居所】　東京都渋谷区桜丘町２９－１０－５０１
　【氏名】　照内　点
【特許出願人】
　【識別番号】　500565917
　【氏名又は名称】　ケープレックス・インク
【代理人】
　【識別番号】　100089705
　【住所又は居所】　東京都千代田区大手町二丁目２番１号　新大手町ビル２０６区　ユアサハラ法律特許事務所
　【弁理士】
　【氏名又は名称】　社本　一夫
　【電話番号】　03-3270-6641
【選任した代理人】
　【識別番号】　100071124
　【弁理士】
　【氏名又は名称】　今井　庄亮
【選任した代理人】
　【識別番号】　100076691
　【弁理士】
　【氏名又は名称】　増井　忠弐
【選任した代理人】
　【識別番号】　100075270
　【弁理士】

【氏名又は名称】　小林　泰

【選任した代理人】

【識別番号】　100096013

【弁理士】

【氏名又は名称】　富田　博行

【手数料の表示】

【予納台帳番号】　051806

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　構造を持った文書に対する電子署名方法及び装置

【特許請求の範囲】

【請求項１】　対象の文書を解析し、構造を持った表現を生成するステップと、生成された各構造要素から電子署名を生成するステップと、生成された電子署名を構造に対応した1つの署名に結合するステップと、
からなる電子署名方法。

【請求項２】　請求項１に記載の方法において、電子署名を付する文書構造のレベルを設定することによって、電子署名の厳密性を可変とすることを特徴とする電子署名方法。

【請求項３】　請求項１又は２に記載の方法において、結合された電子署名の全体で対象文書の全体を表現するものとし、その全体に対する各構造の電子署名の正否の割合から、対象文書の正否の度合いを表現することによって、対象文書の一致率を表現することを特徴とする電子署名方法。

【請求項４】　請求項１、２又は３に記載の方法において、前記結合するステップが、生成された電子署名を列挙することであることを特徴とする電子署名方法。

【請求項５】　対象文書を解析し、構造を持った表現とするための手段と、生成された各構造要素から署名を生成する手段と、
生成された署名を構造に対応した1つの署名に結合するための手段と、
を含む電子署名装置。

【請求項６】　請求項５に記載の装置において、前記電子署名生成手段において電子署名を付する文書構造のレベルを設定可能とすることによって、電子署名の厳密性を可変とすることを特徴とする電子署名装置。

【請求項７】　請求項５又は６に記載の装置において、前記結合する手段が、生成された電子署名を列挙することを特徴とする電子署名装置。

【請求項８】　請求項５、６又は７に記載の装置において、更に、
生成された電子署名を持った対象文書を検証するための、対象文書の構造を解析する手段と、各構造毎に電子署名を解析する手段とを有することを特徴とする

電子署名装置。

【請求項９】　請求項８に記載の装置において、前記電子署名を解析する手段が、結合された電子署名全体で対象文書の全体を表現するものとし、その全体に対する各構造の電子署名の正否の割合から、対象文書の正否の度合いを表現することによって、対象文書の一致率を決定することを特徴とする電子署名装置。

【請求項１０】　対象文書を解析し、構造を持った表現を生成する手段と、生成された各構造要素から電子署名を生成する手段と、生成された電子署名を構造に対応した1つの署名に結合する手段とを含む、電子署名生成装置と、

生成された電子署名を持った対象文書の構造を解析する手段と、付加された電子署名を解析する手段とを含む、電子署名解析装置と、

からなる電子署名装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子ファイルの正しさを保証するために利用する電子署名技術に関し、特に、構造を持った文書を内容とする電子ファイルに対する電子署名技術に関する。

【０００２】

【従来の技術】

電子署名技術は、電子ファイルの内容が、電子署名を施した以後修正されていないことを保証するために、暗号化技術を利用するものである。このため、例えば電子ファイル又はそのダイジェストを暗号化し、その暗号化された値をもとの電子ファイルと共に送り、受け取り側で復号した値と、もとの電子ファイル又はそのダイジェストとが等しいことにより、内容の修正がないことを保証している。

【０００３】

しかし、上記のような従来の電子署名技術では、電子ファイル全体として内容の等価性を保証することは可能であるが、電子ファイルの内容が構造を持った文書である場合に、その構造についての等価性を表現することは不可能であった。

【０００４】

このため、ファイルとしては等価ではないが、文書構造は等価であるという状況であっても、内容が異なるという情報しか得ることができないため、このような状況を把握することはできなかった。

【０００５】

また、等価か否か、という２種類の表現しかできなかったため、等価でない場合に、構造上どこが、あるいは、どの程度異なるのかを表現することはできなかった。

【０００６】

【発明が解決しようとする課題】

以上のような状況に鑑み、本発明は、構造を持った文書を内容とする電子ファイルに対する電子署名技術であって、電子ファイルにおける等価性、文書構造における等価性、文書構造における一部の等価性という等価性のレベルを設定評価可能な電子署名技術を提供することを目的とする。

【０００７】

【課題を解決するための手段】

前記の目的を実現するため、本発明は、構造を持った文書を内容とする電子ファイルに対する電子署名方法及び装置であって、対象文書の各構造要素より署名を生成する方法及び装置を提供する。

【０００８】

本発明の電子署名方法は、対象文書を解析し、構造を持った表現を生成する。次に生成された各構造要素から署名を生成し、生成された署名(暗号)を構造に対応した1つの署名に結合する。各構造要素から暗号を生成する方法としては特定の方式に限定されることなく、一般的な暗号生成方法を利用することが可能である。

【０００９】

また、本発明の電子署名方法は、生成された電子署名を持った電子ファイルを検証して、処理の要求に応じ、少なくとも（１）電子ファイルとしての等価性と、（２）文書構造としての等価性と、（３）一致率とを、署名内容から導出する

【００１０】

本発明の電子署名装置は、図１に示すように電子署名生成装置１１と、電子署名解析装置１２とを含み、電子署名生成装置１１は、対象文書１３を解析し、構造を持った表現とするためのパーザ部１４と、該パーザ部１４により生成された各構造要素から署名を生成する暗号生成部１５と、生成された署名(暗号)を構造に対応した1つの署名に結合するための署名生成部１６を含む。

【００１１】

また、電子署名解析装置１２は、生成された電子署名を持った電子ファイル１７を検証するために、同様にパーザ部１８、および、署名解析部１９を有する。該署名解析部１９は、処理の要求２０に応じ、少なくとも（１）電子ファイルとしての等価性の検証２１と、（２）文書構造としての等価性の検証２２と、（３）一致率の導出２３の３つの機能を有する。

【００１２】

【実施例】

まず本発明方法及び装置が対象とする「構造を持った文書」について説明する。通常の文書は、章や節、段落という構造を持っており、これを図に表わすと図２に示すような木構造とすることができる。本発明の電子署名方法及び装置はこの様な木構造として表わすことの可能な文書を内容とする電子ファイルを対象とする。

【００１３】

このような構造を持った文書の例として、ＸＭＬによって記述されたファイルがあり、その様なＸＭＬファイルの一例を図３に示す。

図示の例では、ＸＭＬの仕様においてホワイトスペース(White Space)という、インデントを表現するためのタブや改行の情報がファイルに含まれているが、ＸＭＬにおいては、文書構造を変更することのない範囲でのホワイトスペースの使用を認めているので、そのような情報が削除されても、文書構造自体に違いは存在しない。その様な、図３と構造的に同一のＸＭＬファイルの例を図４に示す。しかし、これらのファイル同士をファイルとして比較した場合は異なるものと

して扱われる。

【００１４】

従来、ＸＭＬにおいて、これらが等価な文書構造であるかどうかは、ＸＭＬパーザ(xml Parser)を用いて解析した結果をＤＯＭオブジェクト(DOM Object)として生成した結果等価であることを判断することではじめて可能となるのであるが、本発明の電子署名方法及び装置を用いると、図３のファイルと図４のファイルは、ファイルを示す署名コードは異なるが、文書構造を示す署名コードは、同じ値となり、ファイル内容としては異なるが、文書構造は等価であることを署名コードにより知ることが可能となる。

【００１５】

これらのファイル及び文書構造についての署名の例を図５に示す。各構造要素を17桁の10進数値へマッピングする暗号化を行った場合、図示のような対応となったとする。次にこれらの暗号情報を元に、署名を生成する。結合方式を図６に示すようなフォーマットとする。図中ファイル署名コードはファイルとしての一致性を示す暗号であり、0xFFは各要素のデリミタである。深さコードは木構造のどの深さまでを署名内に含むかを示す数値である。深さコードが0の場合、全ての深さを含むものとする。ノード署名コードは、各要素のコードである。これを構成要素に追加することで、図７に示すような電子署名付き文書となる。図７に示す例では、<Signature>…</Signature>というSignatureノードを追加し、署名の構成をわかりやすいように、文字列連結として"+"記号を使って署名連結を示している。実際には、その結合結果が署名となる。

【００１６】

本発明による電子署名装置は、図８に示すようなＣＰＵ８１、記憶装置８２、ファイルシステム８３、表示装置８４及び入力装置８５を有するコンピュータシステム８６上に構築されても良い。ファイルシステム８３には本発明の電子署名をデータとしてもった構造文書が保存/管理される。本発明においては、その文書の所在は特定しないため、データがデータベースに置かれる場合もある。

【００１７】

このようなシステム構成において、本発明による電子署名方法及び装置は、フ

ファイルシステム８３に保存されているファイルを、構造を持った文書として扱い、不正な修正が加えられていないかどうか、さらに修正されていれば、どの構造部分が修正されているかを検証することができる。

【００１８】

この検証の例として、ファイルのどの部分が修正されているかを検証することによって、システムの不正動作を予防する応用を示す。

この応用例は、データベースへ接続する設定を自動生成するツールが、電子署名を含んだファイルを生成することによって、不正な修正に対して、データベースへ接続する以前に、修正された個所を指摘し、ユーザに注意を促すものである。

【００１９】

従来データベースへ接続する設定を自動生成するツールにより自動的に生成される設定ファイルは、そのツール以外の別の方法による修正をサポート範囲外とするが、通常そのような別の方法による修正を加えられたかどうかを示す情報はファイルに付加されない。また、仮にこの様な設定ファイルに従来の電子署名を付加したとしても、修正されたことしか判別できず、修正個所は不明である。また、ファイルとしての修正のみの検証であるため、構造情報上、動作に不都合がない修正の場合でも、不正であることを示すのみで、適切かつ十分な処理とはいえない。

【００２０】

この応用例のシステム構成を図９に示す。このシステムは図８に示したシステムにデータベースシステム９１を追加したものであり、図８と同じ参照番号は同じ構成要素を示す。データベースシステム９１を接続するためには、設定を行わなければならないが、このシステムでは、それらの設定をユーザと対話的に自動生成するツール(ConfigGenTool)９２を更に有する。このツール９２は、データベースシステムに接続するための情報をユーザに入力してもらいそれらの情報から設定ファイルを生成するツールであって、その設定により、データベースシステム９１へ接続可能なことを検証して、設定ファイル(Config.xml) ９３を生成する。設定ファイル９３の生成時に、本発明による電子署名を付加するかどうか

を指示することが可能であり、その厳密性をユーザが選択することができる。図１０に電子署名を付加した設定ファイル９３の例を示す。ここでは、各構造要素や、ファイル自身の署名は１７桁の１６進数表現で構成されている。

【００２１】

この様にして生成された設定ファイル９３は、実際にシステムがデータベースシステム９１にアクセスする時に起動されるデータベースシステムアクセスモジュール(DBAccessor)９４によって参照される。このときモジュール９４は、設定ファイル９３に電子署名が含まれる場合、その正当性をアクセス前に検証する。設定ファイル９３が図１１に示すように変更されている場合、モジュール９４は、このファイルがファイル一致性については不正であるが、構造としては本のファイルと一致しているため、通常通りのデータベースアクセス処理を行う。即ちこの図１０から図１１への修正は、ＸＭＬの仕様のホワイトスペースであるタブ、改行コードが削除されただけなので、ＸＭＬとしては等価である。

【００２２】

また、設定ファイル９３が図１２の下線部に示すように変更されている場合、モジュール９４は、アクセス処理を開始する前に、このファイルの不一致の場所を特定して「指定されているプロバイダが不正です」という旨のメッセージをユーザに対して表示することが可能である。このように、データベースシステムへのアクセス設定ファイルに本発明の電子署名を利用すると、変更されたことにより不正となっている部分を動作させることなく指摘して不正なアクセスを回避することが可能である。

【００２３】

更に、本発明の電子署名方法及び装置を用いると、前述のように構造を有する文書を内容とする電子ファイルの各構造毎に一致、不一致を判定できるので、構造全体に対する一致率又は不一致率を計算することができ、その値によってシステムの動作を制御することも可能になる。

【００２４】

【発明の効果】

本発明による電子署名方法及び装置を用いることによって、電子署名を抽出比

較することで、構造を持った文書を内容とする電子ファイルの、ファイルとしての等価性の検証と、文書構造としての等価性の検証と、それらの一致率の導出をすることが可能となる。

【図面の簡単な説明】

【図１】　電子署名装置及び処理の流れを示す概念図。

【図２】　文書の木構造を示す図。

【図３】　ＸＭＬファイルの構造を例示する図。

【図４】　ＸＭＬとしては等価な異なるファイルの構造を例示する図。

【図５】　文書と各要素の暗号対応を示す図。

【図６】　電子署名の結合フォーマットを例示する図。

【図７】　電子署名付きＸＭＬファイルを示す図。

【図８】　本発明を実施するシステム構成例を示す図。

【図９】　応用例のシステム構成例を示す図。

【図１０】　電子署名を付加した設定ファイルの例を示す図。

【図１１】　設定ファイルの変更例を示す図。

【図１２】　設定ファイルの別の変更例を示す図。

【符号の説明】

１１：電子署名生成装置

１２：電子署名解析装置

１３：対象文書

１４，１８：パーザ部

１５：暗号生成部

１６：署名生成部

１７：署名付電子ファイル

１９：署名解析部

２０：処理要求

２１：ファイル検証

２２：文書構造検証

２３：一致率導出

８１：ＣＰＵ

８２：記憶装置

８３：ファイルシステム

８４：表示装置

８５：入力装置

８６：コンピュータシステム

９１：データベースシステム：

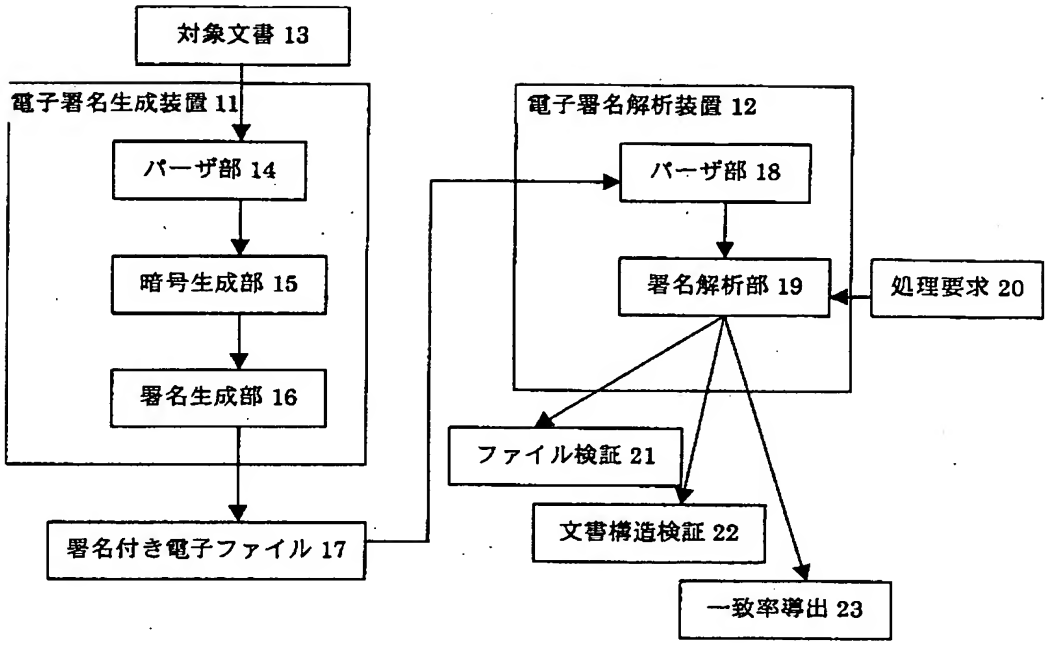
９２：設定ファイル生成ツール

９３：設定ファイル

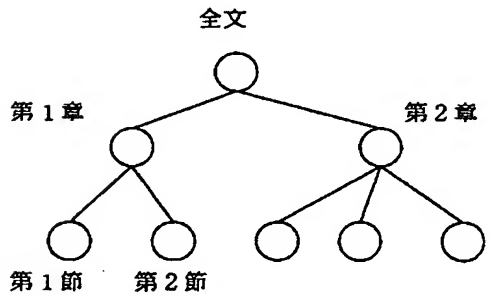
９４：データベースシステムアクセスモジュール

【書類名】　図面

【図１】


対象文書 13
電子署名生成装置 11
パーザ部 14
暗号生成部 15
署名生成部 16
署名付き電子ファイル 17
電子署名解析装置 12
パーザ部 18
署名解析部 19
処理要求 20
ファイル検証 21
文書構造検証 22
一致率導出 23

【図２】


全文
第１章
第２章
第１節
第２節

【図３】

```
<? xml version=" 1.0"  encoding=" utf-8"  ?>
<Document>
        <第１章>
                <第１節>…</第１節>
                <第２節>…</第２節>
        </第１章>
        <第２章>
                <第１節>…</第１節>
                <第２節>…</第２節>
                <第３節>…</第３節>
        </第２章>
</Document>
```

【図４】

```
<? xml version=" 1.0"  encoding=" utf-8"  ?>
<Document><第１章><第１節>…</第１節><第２節>…</第２節></第１章>
<第２章><第１節>…</第１節><第２節>…</第２節><第３節>…</第３節></第２章>
</Document>
```

【図５】

```
<? xml version=" 1.0"  encoding=" utf-8"  ?>
<Document>
        <第１章>  ------------------------> 01424442344553994
                <第１節>…</第１節>---------> 10458043242424234
                <第２節>…</第２節>---------> 15357989849284423
        </第１章>
        <第２章> ------------------------> 01643544098078423
                <第１節>…</第１節>---------> 10572839792742349
                <第２節>…</第２節>---------> 17932032304804822
                <第３節>…</第３節>---------> 15239759890098203
        </第２章>
</Document>
```

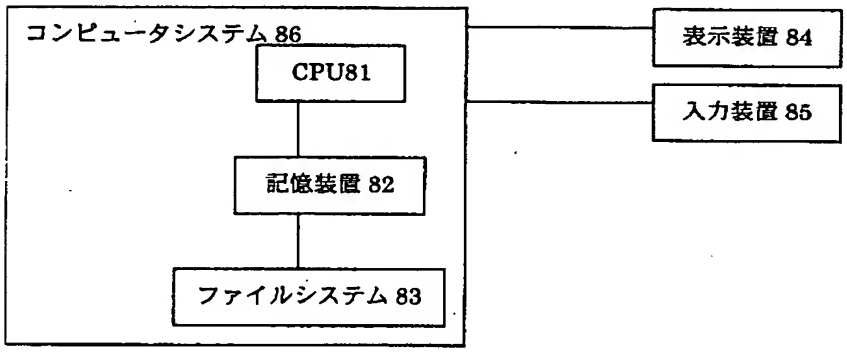
【図６】

ファイル署名コード	0xFF	深さコード	0xFF	ノード署名コード(1)	0xFF	ノード署名コード(2)	…

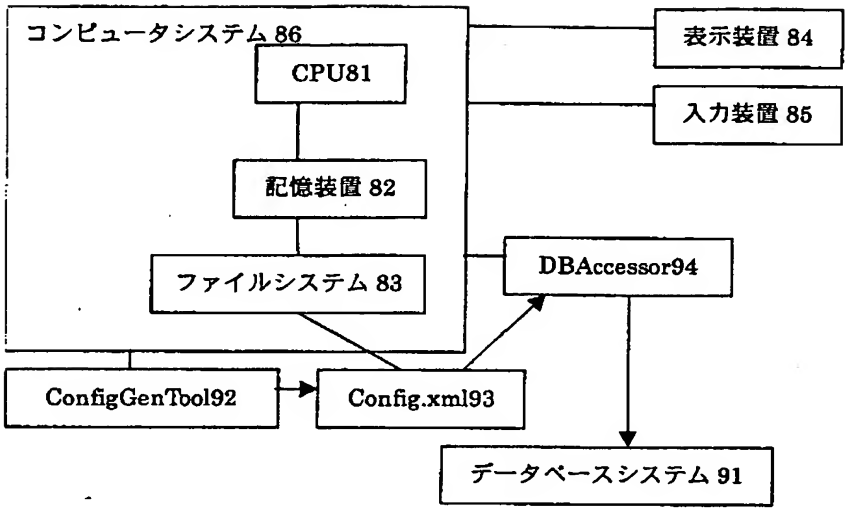
【図７】

```
<? xml version=" 1.0"  encoding=" utf-8"  ?>
<Document>
        <第１章>
                <第１節>…</第１節>
                <第２節>…</第２節>
        </第１章>
        <第２章>
                <第１節>…</第１節>
                <第２節>…</第２節>
                <第３節>…</第３節>
        </第２章>
        <Signature>31233123125443242+0xFF+0x00+014244423445539 94+0xFF+
104580432424234+0xFF+15357989849284423+0xFF+01643544098078423+0xFF+1
0572839792742349+0xFF+17932032304804822+0xFF+15239759890098203</Signat
ure>
</Document>
```

【図８】



【図９】



【図１０】

```
<?xml version="1.0" encoding="utf-8"?>
<OLEDBSetting>
        <Provider>SQLOLEDB.1</Provider>
        <IntegratedSecurity>SSPI</IntegratedSecurity>
        <PersistSecurityInfo>False</PersistSecurityInfo>
        <InitialCatalog>Northwind</InitialCatalog>
        <DataSource>DARKSTAR</DataSource>
        <UseProcedureforPrepare>1</UseProcedureforPrepare>
        <AutoTranslate>True</AutoTranslate>
        <PacketSize>4096</PacketSize>
        <WorkstationID>DARKSTAR</WorkstationID>
        <Signature>032423afb432ef432ff00ff153453adb432e532ff
f1443f0988fe080809ff153452f4b2ed42304ff1543409888d8eba34ff10
98043242a988edbff1143298ef0a0b0cd0ff18aaadbc443298753ff15432
42d9009e7bc3ff125438a0f0d0e0083</Signature>
</OLEDBSetting>
```

【図１１】

```
<?xml version="1.0" encoding="utf-8"?>
<OLEDBSetting><Provider>SQLOLEDB.1</Provider><IntegratedSecu
rity>SSPI</IntegratedSecurity><PersistSecurityInfo>False</Pe
rsistSecurityInfo><InitialCatalog>Northwind</InitialCatalog>
<DataSource>DARKSTAR</DataSource><UseProcedureforPrepare>1</
UseProcedureforPrepare><AutoTranslate>True</AutoTranslate><P
acketSize>4096</PacketSize><WorkstationID>DARKSTAR</Workstat
ionID><Signature>032423afb432ef432ff00ff153453adb432e532fff1
443f0988fe080809ff153452f4b2ed42304ff1543409888d8eba34ff1098
043242a988edbff1143298ef0a0b0cd0ff18aaadbc443298753ff1543242
d9009e7bc3ff125438a0f0d0e0083</Signature>
</OLEDBSetting>
```

【図１２】

```
<?xml version="1.0" encoding="utf-8"?>
<OLEDBSetting>
        <Provider>Microsoft.Jet.OLEDB.4.0</Provider>
        <IntegratedSecurity>SSPI</IntegratedSecurity>
        <PersistSecurityInfo>False</PersistSecurityInfo>
        <InitialCatalog>Northwind</InitialCatalog>
        <DataSource>DARKSTAR</DataSource>
        <UseProcedureforPrepare>1</UseProcedureforPrepare>
        <AutoTranslate>True</AutoTranslate>
        <PacketSize>4096</PacketSize>
        <WorkstationID>DARKSTAR</WorkstationID>
        <Signature>032423afb432ef432ff00ff153453adb432e532ff
f1443f0988fe080809ff153452f4b2ed42304ff1543409888d8eba34ff10
98043242a988edbff1143298ef0a0b0cd0ff18aaadbc443298753ff15432
42d9009e7bc3ff125438a0f0d0e0083</Signature>
</OLEDBSetting>
```

【書類名】　　要約書

【要約】

【課題】

構造を持った文書を内容とする電子ファイルに対する電子署名技術であって、電子ファイルにおける等価性、文書構造における等価性、文書構造における一部の等価性という等価性のレベルを設定評価可能な電子署名技術を提供する。

【解決手段】

対象文書を解析し、構造を持った表現を生成する。次に生成された各構造要素から署名を生成し、生成された署名(暗号)を構造に対応した1つの署名に結合する。また、生成された電子署名を持った電子ファイルを検証して、処理の要求に応じ、少なくとも（１）電子ファイルとしての等価性と、（２）文書構造としての等価性と、（３）一致率とを、署名内容から導出する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔５００５６５９１７〕

１．変更年月日　　２０００年１２月２７日
［変更理由］　名称変更
住　所　　アメリカ合衆国カリフォルニア州９５１１０，サン・ホセ，ゲイトウェイ・プレイス　２０３３，スイート　５００
氏　名　　ケープレックス・インク